FI > DT
10-4-02

PATENT
Customer No. 22,852
Attorney Docket No. 4284.0856

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

ATSUSHI SHIMBO

Application No.: 10/051,280

Filed: January 22, 2002

For: MODULAR ARITHMETIC APPARATUS AND METHOD SELECTING A BASE IN THE RESIDUE NUMBER SYSTEM

Group Art Unit: 2121

Examiner: Unknown

Commissioner for Patents
Washington, DC 20231

CLAIM FOR PRIORITY

Sir:

Under the provisions of Section 119 of 35 U.S.C., Applicant hereby claims the benefit of the filing date of Japanese Patent Application Number 2001-013564, filed January 22, 2001, for the above identified United States patent application.

In support of Applicant's claim for priority, a certified copy of the priority application is filed herewith.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.

Dated: Oct. 1, 2002

By: Richard V. Burgujian Reg No 24,014
for Reg. No. 31,744

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

901 I Street, NW
ton, DC 20005
08.4000
08.4400
an.com

【書類名】　特許願
【整理番号】　A000007704
【提出日】　平成13年 1月22日
【あて先】　特許庁長官　殿
【国際特許分類】　G09C　1/00
【発明の名称】　剰余系表現を利用した演算装置及び方法及びプログラム
【請求項の数】　9
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
【氏名】　新保　淳
【特許出願人】
【識別番号】　000003078
【氏名又は名称】　株式会社　東芝
【代理人】
【識別番号】　100058479
【弁理士】
【氏名又は名称】　鈴江　武彦
【電話番号】　03-3502-3181
【選任した代理人】
【識別番号】　100084618
【弁理士】
【氏名又は名称】　村松　貞男
【選任した代理人】
【識別番号】　100068814
【弁理士】
【氏名又は名称】　坪井　淳
【選任した代理人】
【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　剰余系表現を利用した演算装置及び方法及びプログラム

【特許請求の範囲】

【請求項１】　法ｐを含むデータを入力し、互いに素なｎ個の整数の組Ａ＝$\{a_1,a_2,\ldots,a_n\}$を基底とする剰余系表現により前記法ｐに対する剰余付きでの整数演算を実行する演算装置において、

前記基底の要素数ｎが異なる複数の基底毎の基底パラメータを記憶する基底パラメータ記憶手段と、

前記入力された法ｐのサイズに応じて、演算装置内で処理に利用する基底を選択する基底選択手段と、

前記基底選択手段により選択された基底に該当する基底パラメータを前記記憶手段から読み出し、該基底パラメータに基づいて基底要素毎の演算を行う複数の演算ユニットと、

具備することを特徴とする剰余系表現を利用した演算装置。

【請求項２】　前記基底パラメータ記憶手段に記憶される要素数ｎは、前記演算ユニット数ｕの倍数であることを特徴とする請求項１に記載の剰余系表現を利用した演算装置。

【請求項３】　前記基底パラメータ記憶手段に記憶される要素数ｎは、演算ユニット数をｕとし、停止させる演算ユニット数の最大値に相当する小さな整数をδ（$0 \leqq \delta < u$）とするとき、ｕ－δ，ｕ－δ＋１，…，ｕのそれぞれの倍数であることを特徴とする請求項１に記載の剰余系表現を利用した演算装置。

【請求項４】　前記基底選択手段は、基底要素の積の値が前記法ｐよりも大きい基底の中で最も積の値が小さい基底を選択することを特徴とする請求項１乃至３のいずれかに記載の剰余系表現を利用した演算装置。

【請求項５】　互いに素なｎ個の整数の組Ａ＝$\{a_1,a_2,\ldots,a_n\}$を基底とする剰余系表現により法ｐに対する剰余付きでの整数演算を実行する演算方法において、

前記基底の要素数ｎが異なる複数の基底毎の基底パラメータを基底パラメータ記憶手段に記憶させておき、

法ｐを含むデータを入力し、

該入力された法ｐのサイズに応じて、演算装置内で処理に利用する基底を選択し、

前記選択された基底に該当する基底パラメータを前記基底パラメータ記憶手段から読み出し、

該読み出された基底パラメータに基づいて、基底要素毎の演算を複数の演算ユニットにより実行することを特徴とする剰余系表現を利用した演算方法。

【請求項６】　前記基底パラメータ記憶手段に記憶される要素数ｎは、前記演算ユニット数ｕの倍数であることを特徴とする請求項５に記載の剰余系表現を利用した演算方法。

【請求項７】　前記基底パラメータ記憶手段に記憶される要素数ｎは、演算ユニット数をｕとし、停止させる演算ユニット数の最大値に相当する小さな整数をδ（０≦δ＜ｕ）とするとき、ｕ－δ，ｕ－δ＋１，…，ｕのそれぞれの倍数であることを特徴とする請求項５に記載の剰余系表現を利用した演算方法。

【請求項８】　前記基底の選択ステップは、基底要素の積の値が前記法ｐよりも大きい基底の中で最も積の値が小さい基底を選択することを特徴とする請求項５乃至７のいずれかに記載の剰余系表現を利用した演算方法。

【請求項９】　互いに素なｎ個の整数の組Ａ＝$\{a_1,a_2,...,a_n\}$を基底とする剰余系表現により法ｐに対する整数演算を行う機能をコンピュータに実現させるためのプログラムにおいて、

前記基底の要素数ｎが異なる複数の基底毎の基底パラメータを基底パラメータ記憶手段に記憶させる機能と、

法ｐを含むデータを入力する機能と、

該入力された法ｐのサイズに応じて、演算装置内で処理に利用する基底を基底選択器に選択させる機能と、

該選択された基底に該当する基底パラメータを前記基底パラメータ記憶手段から読み出す機能と、

該読み出された基底パラメータに基づいて、基底要素毎の演算を複数の演算ユニットに実行させる機能と、を具備することを特徴とするプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、剰余系（ＲＮＳ；Residue Number System）表現を利用した演算装置に関する。

【０００２】

【従来の技術】

大きな整数を効率良く演算するための手法として知られる剰余演算系においては、互いに素な比較的小さな整数の組$\{a_1, a_2, \cdots, a_n\}$を用意し、表現対象となる大きな整数をこれらの整数で割った余りで表現する。以後、この整数の組を剰余演算系の基底(base)と称する。また、要素数ｎを基底数（又は基底サイズ）と称する。

【０００３】

例えば基底$\{a_1, a_2, \cdots, a_n\}$が与えられている場合、整数ｘは、これを基底$a_i$(i=1,2,...,n)で除して得られるｎ個の余り$\{x_1, x_2, \cdots, x_n\}$により表現される。このとき、数xが基底要素の積Ａ($=a_1a_2\cdots a_n$)未満の正整数であれば、数ｘは基底要素の積Ａを法として一意に表現できる。言いかえれば、数ｘとその剰余演算系表現$\{x_1, x_2, \cdots, x_n\}$は一対一に対応する。

【０００４】

このような剰余演算系表現において２つの整数x, yの積を計算するには、まず、各要素毎の積を求め、さらに、対応する基底a_iで除した余りを求める。これは、一般的には、各要素毎に対応する基底a_iを法とする積を計算することで基底要素の積Ａを法とする積が求められることと言い換えられる。加算および減算についても同様であり、基底a_iに対応する要素x_i, y_iについて、a_iを法とする加算あるいは減算をすればよい。

【０００５】

このような剰余演算系を用いた演算では、乗算・加算・減算は、各要素毎独立に対応する基底を法とする演算を行えば良いのであるが、例えば基底として計算機のワード長以内の値を採用することで、非常に大きな整数の演算を単精度の演

算の繰り返しによって実現できる。

【０００６】

大きな整数同士の演算（加減乗算）の高速な並列処理を可能にするこのような剰余演算系をベースに、公開鍵暗号の基本演算であるべき乗剰余演算（及び剰余乗算）をモンゴメリ乗算との融合により実現するアルゴリズム、およびそのハードウェア構成（「ＲＮＳモンゴメリ乗算器」という）が提案されている。

【０００７】

ＲＮＳモンゴメリ乗算のアルゴリズムについては、については、Kawamura, S., Koike, M., Sano, F. and Shimbo, A, "Cox-Rower Architecture for Fast Montgomery Multiplication", Lecture Notes in Computer Science 1807, Advances in Cryptology - EUROCRYPT2000, pp. 523-538, 2000の記載を参考にできる。

【０００８】

ＲＮＳモンゴメリ乗算器は、剰余系表現で整数を表すために基底を用いる。基底は、演算ワード長と等しいサイズの小整数の組からなり、これら基底の要素の積は、公開鍵暗号のブロックサイズ（例えば１０２４ビット）以上のサイズになっている必要がある。

【０００９】

また、ＲＮＳモンゴメリ乗算器が備える演算ユニット数を、基底要素の数に一致させたり、あるいはその約数にすることで一つの演算ユニット当り複数の基底要素に対応する処理を実行させる方法も提案されている。

【００１０】

ＲＮＳモンゴメリ乗算の計算量は、利用する基底サイズｎの２乗に比例する。また、ＲＮＳモンゴメリ乗算を利用したべき乗剰余計算（ＲＳＡ処理）の計算量は、べき指数のビット長に比例した回数だけＲＮＳモンゴメリ乗算を実行する計算量に相当する。

【００１１】

【発明が解決しようとする課題】

公開暗号では、鍵長は必ずしも固定ではない。これは、セキュリティの強度と

解読技術の進展などに起因する。このため、一つのハードウェアで複数の鍵長に対応する必要がある。

【００１２】

ハードウェアへの実装においては、そのハードウェアに搭載される演算ユニット数が固定され、これに伴い同時に動作する演算ユニット数の上限が定まる。このため、扱う鍵長に応じて、ハードウェアに搭載する演算ユニット数を適切な数に選んでおく必要がある。

【００１３】

最大の鍵長に対応した基底要素数の演算ユニットを用意した場合、単純に鍵長を変えてべき乗剰余算を実行すると、べき指数が短くなる分だけ計算量が減り、処理時間を短縮できる。しかしながら、２進数表現を利用した場合のべき乗剰余算の計算量はビットサイズ（鍵長）の３乗に比例し、計算のオーダーが大きく異なることを勘案すると、この場合の処理時間の短縮効果は十分でない。

【００１４】

また、演算ユニットのワードサイズが３２ビットの場合、ＲＳＡ(Rivest-Shamir-Adleman)のような公開鍵暗号処理において鍵長２０４８ビットに対応するためには６５個の基底要素が必要になる。最大の鍵長に対応した基底要素数を用意する方法では、例えば鍵長５１２ビットのべき乗剰余演算についても６５個の基底要素を使って計算することになり、効率的でない。

【００１５】

しかしながら、従来、異なる鍵長に対応して効率的に処理を行える演算装置の構成は提供されていない。

【００１６】

本発明はこのような事情を考慮してなされたものであり、ハードウェア実装における影響が少なく、かつ鍵長に応じて処理時間の縮小効果が高い剰余系表現を利用した演算装置を提供することを目的とする。

【００１７】

【課題を解決するための手段】

上記課題を解決するために本発明は次のように構成されている。

【００１８】

本発明の請求項１に係る剰余系表現を利用した演算装置は、法ｐを含むデータを入力し、互いに素なｎ個の整数の組Ａ＝｛a_1,a_2,...,a_n｝を基底とする剰余系表現により前記法ｐに対する剰余付きでの整数演算を実行する演算装置において、前記基底の要素数ｎが異なる複数の基底毎の基底パラメータを記憶する基底パラメータ記憶手段と、前記入力された法ｐのサイズに応じて、演算装置内で処理に利用する基底を選択する基底選択手段と、前記基底選択手段により選択された基底に該当する基底パラメータを前記記憶手段から読み出し、該基底パラメータに基づいて基底要素毎の演算を行う複数の演算ユニットと、具備することを特徴とする剰余系表現を利用した演算装置である。

【００１９】

本発明の請求項５に係る演算方法は、互いに素なｎ個の整数の組Ａ＝｛a_1,a_2,...,a_n｝を基底とする剰余系表現により法ｐに対する剰余付きでの整数演算を実行する演算方法において、前記基底の要素数ｎが異なる複数の基底毎の基底パラメータを基底パラメータ記憶手段に記憶させておき、法ｐを含むデータを入力し、該入力された法ｐのサイズに応じて、演算装置内で処理に利用する基底を選択し、前記選択された基底に該当する基底パラメータを前記基底パラメータ記憶手段から読み出し、該読み出された基底パラメータに基づいて、基底要素毎の演算を複数の演算ユニットにより実行することを特徴とする剰余系表現を利用した演算方法である。

【００２０】

本発明の請求項９に係るプログラムは、互いに素なｎ個の整数の組Ａ＝｛a_1,a_2,...,a_n｝を基底とする剰余系表現により法ｐに対する整数演算を行う機能をコンピュータに実現させるためのプログラムにおいて、前記基底の要素数ｎが異なる複数の基底毎の基底パラメータを基底パラメータ記憶手段に記憶させる機能と、法ｐを含むデータを入力する機能と、該入力された法ｐのサイズに応じて、演算装置内で処理に利用する基底を基底選択器に選択させる機能と、該選択された基底に該当する基底パラメータを前記基底パラメータ記憶手段から読み出す機能と、該読み出された基底パラメータに基づいて、基底要素毎の演算を複数の演算

ユニットに実行させる機能と、を具備することを特徴とするプログラムである。

【００２１】

【発明の実施の形態】

以下、図面を参照しながら本発明の実施形態を説明する。

【００２２】

図１は、本発明の剰余系表現を利用した演算装置の一実施形態に係るＲＮＳモンゴメリ乗算器のハードウェア構成を示す回路図である。

【００２３】

剰余演算機能付き積和回路１０１、ＲＡＭ１２１、ＲＯＭ１３１は１つの演算ユニットを構成し、同様の構成の演算ユニットがｎ個並列に並ぶ構成になっている。各演算ユニットの積和回路１０１は、対応する基底要素についてｗビットの演算を行うよう構成されており、各演算ユニットはｗビットのバスによって相互に接続されている。補正計算器１１０は、ＲＮＳモンゴメリ乗算の内部で必要となる基底変換処理における補正項の計算に必要なユニットである。

【００２４】

一つの積和回路１０１は、ＲＡＭ１２１およびＲＯＭ１３１からのデータを入力し、補正計算器１１０からの制御を受けて剰余演算部を行い、その計算結果をｗビットのバスを介してＲＡＭ１２１に送る。

【００２５】

このような構成に加え、本実施形態の装置は、Ｉ／Ｏ部１０に接続され、該Ｉ／Ｏ部１０から法ｐの値を入力し、この法ｐのサイズに応じて、演算装置内で処理に利用する基底を選択する基底選択器２０が付加されている。また、基底の要素数ｎが異なる複数の基底毎の基底パラメータをＲＯＭ１３１が記憶保持しており、個々の演算ユニットは、基底選択器２０により選択された基底に対応する基底パラメータに基づいて動作するように構成されている。

【００２６】

図２は、ＲＯＭに記憶保持される基底パラメータを示す図である。例えば本例では、異なる基底に該当する基底パラメータを選択可能となっており、ＲＯＭ１３１内のアドレス１に基底１パラメータ、アドレス２に基底２パラメータ、…と

いう具合に各基底パラメータが配置されている。これら基底パラメータは、それぞれ、基底数ｎ１，基底数ｎ２，…という具合に基底数が異なる。基底選択器２０は、選択した基底に該当する基底パラメータのＲＯＭ１３１内におけるアドレス１～４のいずれかを出力する。

【００２７】

基底選択器２０における基底の選択基準は、基底要素の積の値が法ｐよりも大きい基底の中で最も積の値が小さい基底、つまり最小の基底数を選択することとする。そして本実施形態では、演算ユニット数の倍数となる基底数に対応した複数の基底パラメータをＲＯＭ１３１に格納しておき、いずれかの基底パラメータを、入力された鍵長（法サイズＬｐ）に応じて選択的に使用する。

【００２８】

図３は、このような基底パラメータの選択のアルゴリズムの一例を説明するためのフローチャートである。

【００２９】

まず、例えばべき乗剰余計算（$y \leftarrow x^e \mod p$）のパラメータとして法ｐを入力する（ステップＳ１）。

【００３０】

次に、入力された法サイズＬｐ（ビット）と、既知である演算ユニットのワードサイズｗ（ビット）及び演算ユニット数ｕの値とに基づいて次式を満たす整数ｉを求める（ステップＳ２）。

【００３１】

【数１】

$$i = \lceil (Lp + w) / (u * w) \rceil \quad (\lceil x \rceil \text{はxの切り上げを表す})$$

【００３２】

次に、ＲＯＭ１３１に記憶されている基底パラメータの基底数のうち、ｎ≧ｉを満たす最小の基底数ｎを選択する（ステップＳ３）。そして、選択された最小の基底数ｎに対応する基底パラメータを選択する。具体的には、基底選択器２０が、選択した基底パラメータのＲＯＭ１３１内のアドレスを出力する（ステップＳ４）。

【００３３】

例えば、演算ユニット数が１１である場合、選択可能な基底数は｛11,22,33,44,55,66,...｝などである。

【００３４】

したがって、現実的なハードウェアへの実装において、例えば図５（ａ）に示すように、法サイズが６７２ビット（ｂｉｔ）以下なら基底数を２２とし、６７２ビットより大きく１０２４ビット以下で基底数を３３とし、１０２４ビットより大きく２０８０ビット以下で基底数を６６とするような、異なる鍵長（法サイズ）に対応した効率的な処理を実現できる。

【００３５】

この例のように法の倍数の基底の一部だけを登録しておくことでも良い。また、例示した表のように法サイズの上限と対応する基底サイズのテーブルを利用して基底選択器を構成してもよい。

【００３６】

本発明に係る演算装置の他の実施形態としては、鍵長で決定される最小の基底数以上の値であって、かつ、基底数を、演算ユニット数を１～最大数までの個々の倍数とした中の最小の値とするように装置構成する。このような基底数に対応した複数の基底パラメータをＲＯＭ１３１に格納しておき、これらの基底パラメータを基底選択器２０が鍵長に応じて選択する。

【００３７】

図４は、このような基底パラメータの選択のアルゴリズムの一例を説明するためのフローチャートである。

【００３８】

まず、例えばべき乗剰余計算（$y \leftarrow x^{e} \mod p$）のパラメータとして法ｐを入力する（ステップＳ１）。

【００３９】

次に、基底数を示す変数ｎ＿Ｆを最大値（無限大）に、変数ｊを（演算ユニット数）ｕ－（最大停止ユニット数）δに初期設定する（ステップＳ２）。

【００４０】

次に、変数ｊが演算ユニット数ｕを超過したか否か（ｊ＞ｕ）を判定し、超過した場合は後述するステップＳ９に移行する（ステップＳ３）。

【００４１】

変数ｊが演算ユニット数ｕを超過しない場合、入力された法サイズＬｐと、既知である演算ユニットのワードサイズｗ及び演算ユニット数ｕの値とに基づいて次式を満たす整数ｉを求める（ステップＳ４）。

【００４２】

【数２】

$$i = \lceil (Lp + w) / (j * w) \rceil \quad (\lceil x \rceil \text{はxの切り上げを表す})$$

【００４３】

次に、ＲＯＭ１３１に記憶されている基底パラメータの基底数のうち、ｎ≧ｉを満たす最小の基底数ｎを選択する（ステップＳ５）。

【００４４】

次に、基底数を示す変数ｎ＿Ｆがステップ５において選択された基底数ｎよりも大きいか否かを判定する（ステップＳ６）。

【００４５】

ステップＳ６においてＹＥＳの場合は、ステップＳ８においてｊを＋１ほどインクリメントしてステップＳ３に戻る。一方、ステップＳ６においてＮＯの場合は、ステップＳ７において基底数を示す変数ｎ＿Ｆを基底数ｎで更新したのち、ステップＳ８においてｊを＋１ほどインクリメントしてステップＳ３に戻る。

【００４６】

ステップＳ９においては、基底数ｎ＿Ｆに対応する基底パラメータのＲＯＭ１３１内のアドレスが出力される。例えば、演算ユニット数が１１であり、最大停止ユニット数δ＝２の場合、選択可能な基底数は｛9,10,11,18,20,22,27,30,33,36,40,44,45,50,55,54,60,66,...｝などである。

【００４７】

したがって、現実的なハードウェアへの実装において、例えば図５（ｂ）に示すように、法サイズが５４４ビットまでなら基底数を１８とし、この場合、演算ユニット数１１のうち、９つのユニットを２回使用することとし、法サイズが５

４４ビットより大きく８３２ビット以下で基底数を２７とし、この場合、演算ユニット数１１のうち、９つのユニットを３回使用することとし、法サイズが８３２ビットより大きく１０２４ビットまでなら基底数を３３とし、この場合、演算ユニット数１１のうちすべてのユニットを３回使用することとし、法サイズが１０２４ビットより大きく１５６８ビット以下なら基底数を５０とし、この場合、演算ユニット数１１のうち、１０個のユニットを５回使用することとし、法サイズが１５６８ビットより大きく２０８０ビット以下なら基底数を６６とし、この場合、演算ユニット数１１のうち、すべてのユニットを６回使用する、といった異なる鍵長（法サイズ）に対応した効率的な処理を実現できる。

【００４８】

この例のように法の倍数の基底の一部だけを登録しておくことでも良い。また、例示した表のように法サイズの上限と対応する基底サイズのテーブルを利用して基底選択器を構成してもよい。

【００４９】

以上説明したように、ＲＯＭ１３１に複数の基底パラメータが備えられており、法サイズに応じて適切な基底（基底パラメータ）を基底選択器２０が選択するので、ハードウェア実装における影響が少なく、かつ鍵長に応じて処理時間の縮小効果が高い剰余系表現を利用したＲＮＳモンゴメリ乗算器を提供できる。

【００５０】

なお、鍵長に依存して決定される最適な基底要素数に対応する演算ユニットだけを利用して処理を行うように構成すれば、計算量がビットサイズの３乗に比例する点で好ましいが、演算ユニットの制御回路が複雑になるという欠点がある。具体的には、演算ユニット数が少ない場合は、演算ユニットを繰り返し利用することで基底全体の処理を行うが、個々の演算ユニットの制御に着目すると、あるタイミングでは動作させ、別のタイミングでは動作させないといった複雑な制御が必要となってしまう。

【００５１】

本発明は上述した実施形態に限定されず種々変形して実施可能である。

【００５２】

【発明の効果】

以上説明したように、本発明によれば、ハードウェア実装における影響が少なく、かつ鍵長に応じて処理時間の縮小効果が高い剰余系表現を利用した演算装置を提供できる。

【図面の簡単な説明】

【図１】

本発明の剰余系表現を利用した演算装置の一実施形態に係るＲＮＳモンゴメリ乗算器のハードウェア構成を示す回路図

【図２】

ＲＯＭに記憶保持される基底パラメータを示す図

【図３】

基底パラメータの選択のアルゴリズムの一例を説明するためのフローチャート

【図４】

基底パラメータの選択のアルゴリズムの他の例を説明するためのフローチャート

【図５】

法サイズの上限と選択される基底数のテーブルによる実現例を示す図

【符号の説明】

１０…Ｉ／Ｏ部

２０…基底選択器

１０１…積和回路

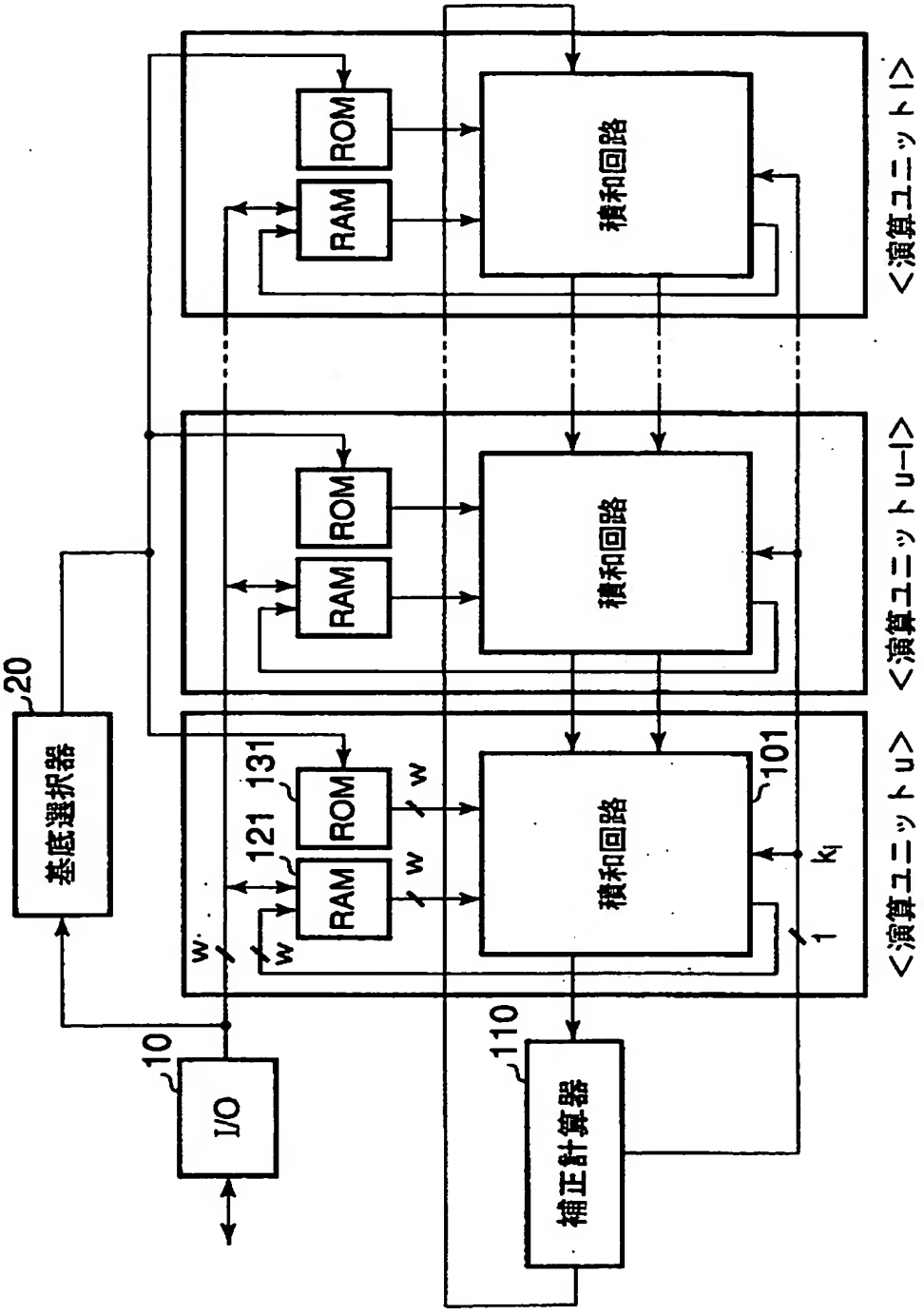
１２１…ＲＡＭ

１３１…ＲＯＭ

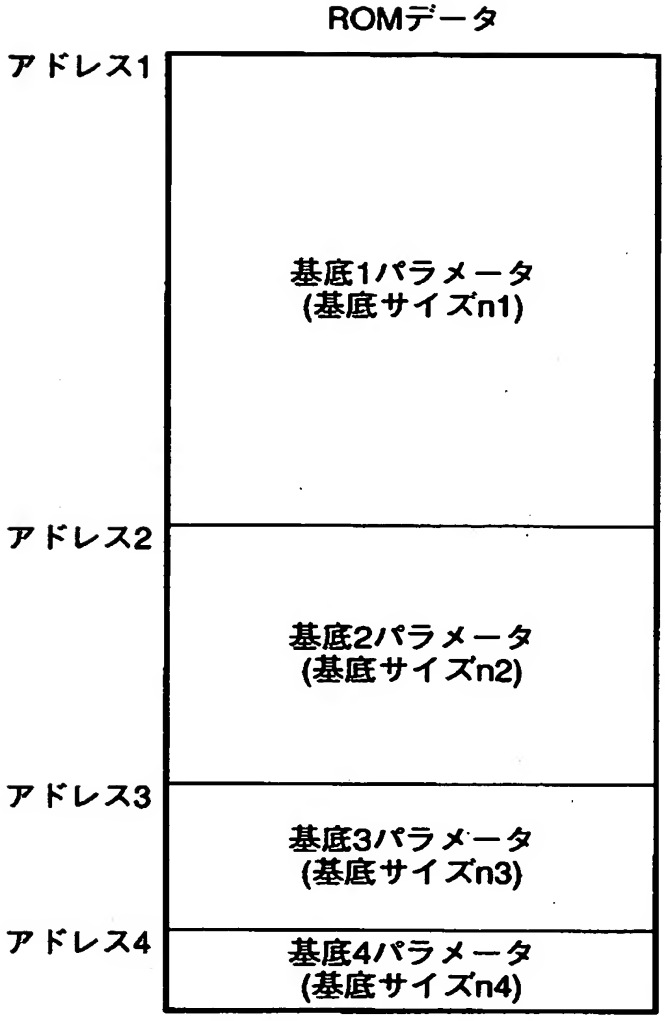
１１０…補正計算器

【書類名】　　図面

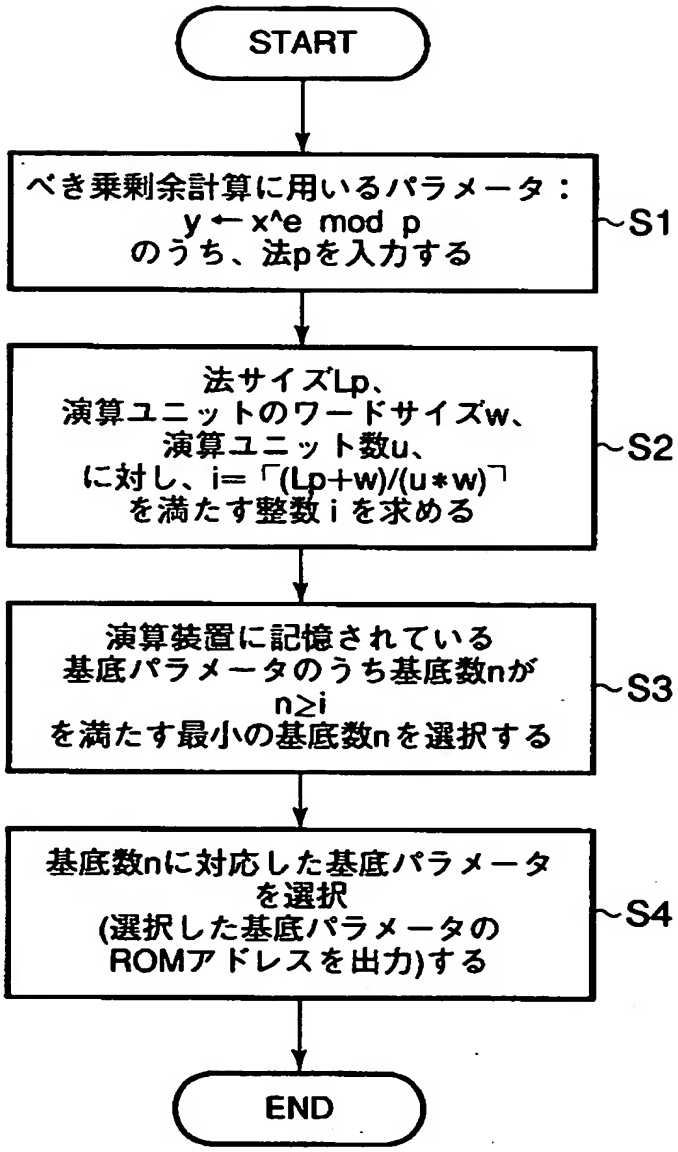
【図１】


ROM
RAM
積和回路
<演算ユニット1>
<演算ユニットu-1>
<演算ユニットu>
基底選択器
20
131
121
101
w
k_l
1
I/O
10
補正計算器
110

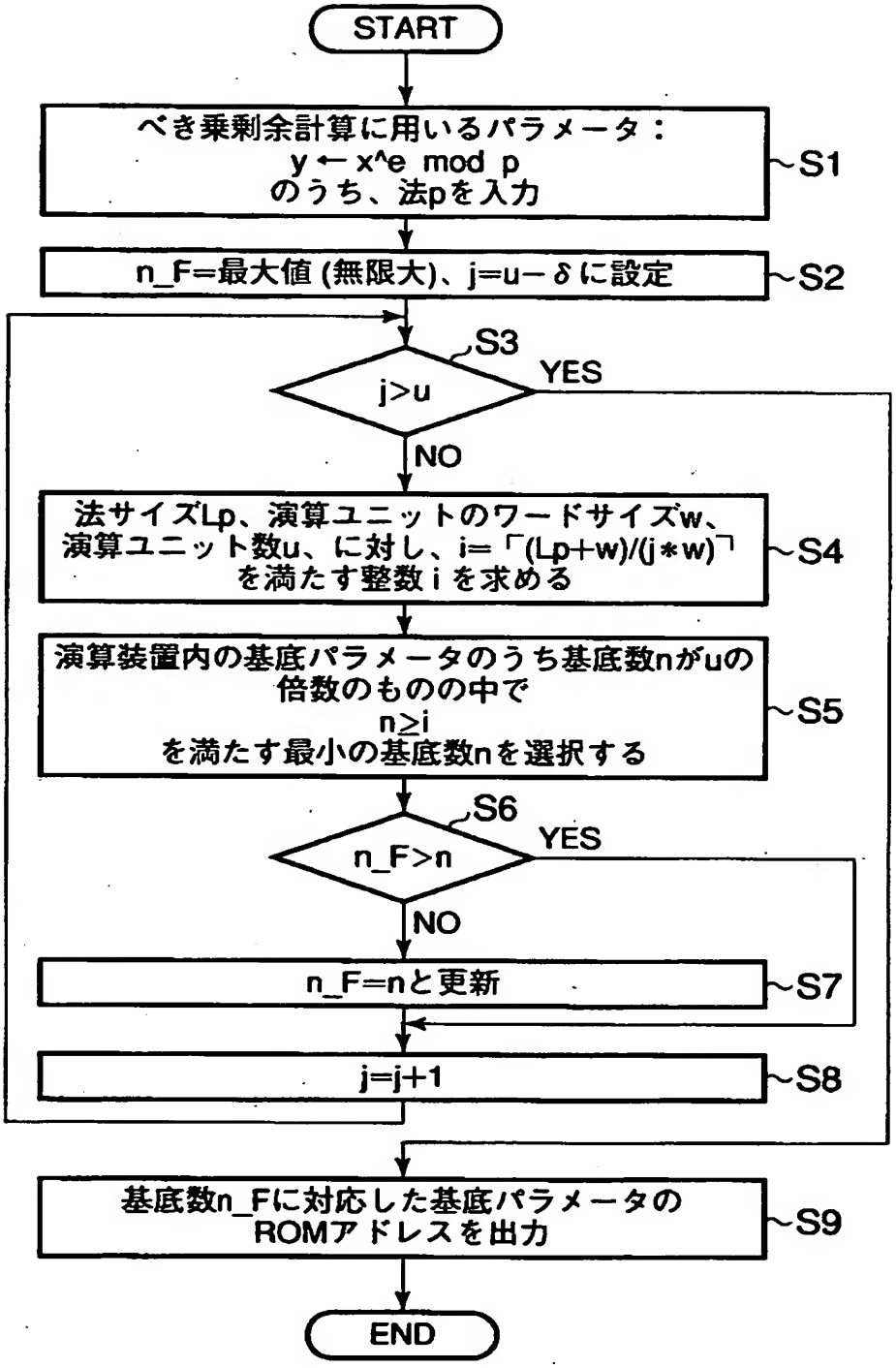
【図２】


ROMデータ
アドレス1
基底1パラメータ
(基底サイズn1)
アドレス2
基底2パラメータ
(基底サイズn2)
アドレス3
基底3パラメータ
(基底サイズn3)
アドレス4
基底4パラメータ
(基底サイズn4)

【図３】


START
べき乗剰余計算に用いるパラメータ：
y←x^e mod p
のうち、法pを入力する
S1
法サイズLp、
演算ユニットのワードサイズw、
演算ユニット数u、
に対し、i=⌈(Lp+w)/(u*w)⌉
を満たす整数 i を求める
S2
演算装置に記憶されている
基底パラメータのうち基底数nが
n≥i
を満たす最小の基底数nを選択する
S3
基底数nに対応した基底パラメータ
を選択
(選択した基底パラメータの
ROMアドレスを出力)する
S4
END

【図４】


START
べき乗剰余計算に用いるパラメータ：
y ← x^e mod p
のうち、法pを入力
S1
n_F=最大値 (無限大)、j=u－δに設定
S2
S3
j>u
YES
NO
法サイズLp、演算ユニットのワードサイズw、
演算ユニット数u、に対し、i=「(Lp+w)/(j*w)」
を満たす整数 i を求める
S4
演算装置内の基底パラメータのうち基底数nがuの
倍数のものの中で
n≧i
を満たす最小の基底数nを選択する
S5
S6
n_F>n
YES
NO
n_F=nと更新
S7
j=j+1
S8
基底数n_Fに対応した基底パラメータの
ROMアドレスを出力
S9
END

【図５】

基底数n	法サイズの上限
22	672bit
33	1024bit
66	2080bit

(a)

基底数n	法サイズの上限
18 (=9unit*2)	544bit
27 (=9unit*3)	832bit
33 (=11unit*3)	1024bit
50 (=10unit*5)	1568bit
66 (=11unit*6)	2080bit

(b)

【書類名】　　要約書

【要約】

【課題】ハードウェア実装における影響が少なく、かつ鍵長に応じて処理時間の縮小効果が高い剰余系表現を利用した演算装置を提供すること

【解決手段】ＲＯＭ１３１に複数の基底パラメータが備えられており、法サイズ（鍵長）に応じて適切な基底（基底パラメータ）を基底選択器２０が選択する。選択された基底パラメータに基づいて基底の各要素に対応する演算ユニットにより剰余付き演算が行われる。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　１９９０年　８月２２日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町７２番地
氏　名　株式会社東芝

２．変更年月日　　２００１年　７月　２日
［変更理由］　住所変更
住　所　東京都港区芝浦一丁目１番１号
氏　名　株式会社東芝

US 1005128006P1

Creation date: 05-11-2004
Indexing Officer: PBOUNMASANONH - PHALYCHANH BOUNMASANONH
Team: OIPEBackFileIndexing
Dossier: 10051280

Legal Date: 11-04-2002

No.	Doccode	Number of pages
1	IDS	3
2	NPL	56

Total number of pages: 59

Remarks:

Order of re-scan issued on .....